CLAIMS:

1. A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of:

configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; and

configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name.

2. The method as recited in claim 1 further comprising the step of:

configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

3. The method as recited in claim 2 further comprising the step of:

activating a particular tunnel of said plurality of tunnels associated with said group name, wherein said particular tunnel is associated with a particular member of said group name.

4. The method as recited in claim 3 further comprising the step of:

transferring data across said particular tunnel.

5. The method as recited in claim 1, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

6. The method as recited in claim 5, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

7. The method as recited in claim 5, wherein said ID is a login ID.

8. The method as recited in claim 5, wherein said ID is a specified name.

9. The method as recited in claim 2, wherein configuring said tunnel definition database in said server node comprises establishing said server node and a client node as the two end points of a particular tunnel.

10. The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

11. The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

12. The method as recited in claim 1, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

13. The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

14. The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.

15. The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

16. The method as recited in claim 1, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

17. The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.

18. The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.

19. The method as recited in claim 3, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of a client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

20. The method as recited in claim 19, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

21. The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

22. The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

23. The method as recited in claim 19, wherein said first ID is an ID of said particular member of said group name.

24. The method as recited in claim 3, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of a client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

25. A network system comprising:

a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises:

a group database, wherein said group database comprises said group name and a list of members associated with said group name; and

a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name.

26. The network system as recited in claim 25, wherein said server node further comprises:

a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

27. The network system as recited in claim 26, wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name.

28. The network system as recited in claim 25, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

29. The network system as recited in claim 28, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

30. The network system as recited in claim 28, wherein said ID is a login ID.

31. The network system as recited in claim 28, wherein said ID is a specified name.

32. The network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

33. The network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

34. The network system as recited in claim 25, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

35. The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

36. The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each

member of said group name and said ID of each member of said group name through a command line interface.

37. The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

38. The network system as recited in claim 25, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

39. The network system as recited in claim 38, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a GUI.

40. The network system as recited in claim 39, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a command line interface.

41. The network system as recited in claim 27, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

42. The network system as recited in claim 41, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

43. The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

44. The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

45. The network system as recited in claim 41, wherein said first ID is an ID of said particular member of said group name.

46. The network system as recited in claim 27, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

47. A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising:

programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; and

programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name.

48. The computer program product as recited in claim 47 further comprises:

programming operable for configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

49. The computer program product as recited in claim 48 further comprises:

programming operable for activating a particular tunnel of said plurality of tunnels associated with said group name, wherein said particular tunnel is associated with a particular member of said group name.

50. The computer program product as recited in claim 49 further comprises:

programming operable for transferring data across said particular tunnel.

51. The computer program product as recited in claim 47, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

52. The computer program product as recited in claim 51, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

53. The computer program product as recited in claim 51, wherein said ID is a login ID.

54. The computer program product as recited in claim 51, wherein said ID is a specified name.

55. The computer program product as recited in claim 48, wherein configuring said tunnel definition database in said server node comprises establishing said server node and a client node as the two end points of a particular tunnel.

56. The computer program product as recited in claim 55, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

57. The computer program product as recited in claim 55, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

58. The computer program product as recited in claim 47, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

59. The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

60. The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.

61. The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

62. The computer program product as recited in claim 47, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

63. The computer program product as recited in claim 62, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.

64. The computer program product as recited in claim 62, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.

65. The computer program product as recited in claim 49, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of a client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

66. The computer program product as recited in claim 65, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

67. The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

68. The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

69. The computer program product as recited in claim 65, wherein said first ID is an ID of said particular member of said group name.

70. The computer program product as recited in claim 49, wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of a client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.